2018-01-01

A national certification programme for academic degrees in cyber security

Furnell, S

10.1007/978-3-319-99734-6_11

IFIP Advances in Information and Communication Technology

A National Certification Programme for Academic Degrees in Cyber Security

Steven Furnell[1], Michael K[2], Fred Piper[3], Chris E2[2], Catherine H2[2], and Chris Ensor[2]

[1] University of Plymouth, Plymouth, United Kingdom
[2] The National Cyber Security Centre, United Kingdom
[3] Codes and Ciphers Limited, Richmond, United Kingdom
sfurnell@plymouth.ac.uk; bachelorscertification@ncsc.gov.uk;
masterscertification@ncsc.gov.uk

Abstract. With a growing need for cyber security skills, there has been a notable increase in the number of academic degrees targeting this topic area, at both undergraduate and postgraduate levels. However, with a widening and varied choice available to them, prospective students and employers require a means to identify academic degrees that offer appropriate and high-quality education in the subject area. This paper presents a case study of the establishment and operation of a certification programme for academic degrees in cyber security. It describes the means by which appropriate topic themes and subject areas for relevant degrees were identified and defined, leading to a certification programme that addresses degrees in general cyber security as well as notable specialisations including digital forensics and network security. The success of the programme is evidenced by 25 degrees across 19 universities having been certified to date, and a continued response to new calls for certification.

Keywords: Certification, Academic Degrees, Bachelor's, Master's, University.

1 Introduction

The cyber security domain is widely-recognised as suffering a skills shortage. For example, a 2013 review by the UK's National Audit Office suggested that it could take up to 20 years to bridge the cyber-skills gap [1], while a 2017 study from (ISC)^2 suggested that the workforce gap could reach 1.8 million by 2022 [2]. As a consequence, the UK's National Cyber Security Strategy identifies the need to strengthen cyber security skills as being a key concern, and highlights a series of systemic issues currently contributing to the shortage [3]:

- the lack of young people entering the profession
- the shortage of current cyber security specialists
- insufficient exposure to cyber and information security concepts in computing courses
- a shortage of suitably qualified teachers
- the absence of established career and training pathways into the profession

It is clear that several of these points relate to academic provision, and the consequent (lack of) supply of qualified graduates to contribute to the discipline. Indeed, further findings from 2017 suggested that only 12% of the UK cyber security workforce is aged under 35 and only 6% of UK companies are hiring appropriately skilled graduates [4]. As such, there is a need to improve the pipeline that higher education can provide, and increase the supply of relevant degree graduates. However, as with security measures themselves, cyber security education is only worthwhile if it is done effectively, and the requirement is more than simply having graduates from degrees that have had superficial coverage of security issues (or worse, had security presented in a manner that is outdated or even incorrect). In this context, it is useful for both prospective students and graduate employers to have a means of identifying credible degrees to match their respective interests and needs. To this end, we present an insight into a successful certification programme that has been introduced by the UK's National Cyber Security Centre (NCSC), including the background and justification for the programme, the design of the certification framework, and some discussion of the experience to date and the related evidence of success.

2 Academic degrees in cyber security

The provision of related degrees in the UK (and indeed internationally) can be traced back to the MSc Information Security, launched by Royal Holloway University of London in 1992 [5]. Since that time, many other degrees have appeared that also target a similar topic space, and the prominence and wider recognition of cyber security in more recent years has arguably served to accelerate this. At the same time, however, it is recognized that some degrees are perhaps more credible than others, and while some are borne out of institutions having a genuine academic presence in the area, others may have been created to capitalize upon the popularity of cyber security. Indeed, one of the main aims of most universities is to offer courses that attract students and one implication of this is that they are attracted to degree titles that receive media attention. Cyber security undoubtedly comes into this category and the growth of degrees that either have the name 'cyber security' or contain cyber security modules has increased dramatically and there are now many alternatives to choose from. For example, at the time of writing, there are in the region of 100 Master's degrees and a slightly larger number of undergraduate degrees in the UK with cyber security or related elements indicated in their titles. There is consequently a need to provide guidance to prospective students and employers on the content and quality of cyber security degrees. Indeed, even where 'security' is in some way present in the degree title, it is not always a guarantee of substantial or sufficient coverage, and an examination of the underlying module/unit titles can sometimes reveal security to be less prominent than might be expected.

Additionally, whilst it may arguably be the case that a university can put together a 'good' syllabus for a degree in cyber security (insofar as they simply need to base it on one that has been published) the quality of the course in practice will depend on the experience of those delivering it. As a baseline, it is therefore important to ensure that the degree content is appropriately matched to the title, *and* that it is supported by a

credible academic base from within which to deliver it, in terms of staff expertise and resourcing [6].

In parallel with the growing range of degrees, the UK Cyber Security Strategy identifies a national requirement for "more talented and qualified cyber security professionals" and this in turn leads to an objective "to ensure the sustained supply of the best possible home-grown cyber security talent" [3]. Such recognition was a driver for the NCSC to establish a certification programme for academic degrees in cyber security. In doing so, the aim is to help set the standard for good cyber security higher education in the UK. Related work has previously been undertaken in the USA, with the National Security Agency and Department of Homeland Security granting Centre of Excellence designations to universities demonstrating their ability to map their curricula to defined knowledge areas in cyber defence [7].

3 Establishing a certification programme

As indicated above, the certification of degrees offers benefits to both students and employers, and should also help universities themselves in attracting both additional numbers and higher quality students into their degrees. The work to set up the UK programme was initiated in 2013, and began with attention towards postgraduate Master's-level degrees. The postgraduate market was seen to offer the most established range of existing degrees named around security in some form (e.g. computer, cyber, information), as well as more specialised titles addressing areas such as digital forensics and network security. In order to approach the certification process in a structured and phased way, it was decided that an initial programme should be established to address Master's degrees seeking to provide a general and broad foundation in cyber security, and then to follow this with later certifications addressing more specialised degrees, as well as to broaden things out to address undergraduate provision.

The initial work to devise the certification framework began in mid-2013, and a fundamental requirement at the outset was to map out each of the supporting disciplines – specifically the broad domains of cyber security and computer science, as well as the specific of topics such as digital forensics and network/Internet security. Rather than attempt to define each of the areas from scratch, it made sense to look at existing categorisations of the topics, and determine the extent to which they were suitable. A number of options were considered from the security perspective, including the main clauses of ISO 27002 (the international code of practice for information security controls) [8] and the eight domains used by the Common Body of Knowledge within the industry-recognised CISSP certification [9]. However, it was ultimately decided that the most suitable foundation would be the Skills Framework from the Institute of Information Security Professionals [10]. This describes the range of competencies expected of information security professionals, and was developed via collaboration between both private and public-sector organisations, academics, and security leaders. Nonetheless, while it was felt to provide a good starting point, the framework was not designed with the certification of academic degrees in mind, and required some refinement for the intended purpose and the type of content that well-regarded security degrees were already seen to be covering. Specifically, it was felt to have an overly gran-

ular emphasis on organisational and managerial aspects of security, while lacking coverage of some key areas on the technical side (e.g. coverage of control systems). This led to some modifications in order to simplify, rebalance, and update the content, and during this period, draft versions of the resulting framework were exposed to external review by a number of stakeholder groups, including government and industry panels, and a wider cross-section of the UK academic community. This ultimately yielded a cyber security subject framework comprising nine Security Disciplines, further subdivided into 14 Skills Groups, as opposed to ten Disciplines and 32 Groups in the IISP original (the top-level security disciplines remained broadly the same as the IISP set, and also adopted the A-J labelling of the disciplines areas themselves – the notable difference was the omission of IISP discipline G – Audit, Assurance & Review – which for the purposes of the NCSC set had been grouped within discipline A on Information Security Management). The full set of resulting disciplines and associated skills groups is listed in Table 1, and as an aside it can be noted that many of the modifications made for the purposes of the degree certification framework were later fed forward into a revised version of the IISP Skills Framework.

For the computer science theme, the choice was more straightforward, as we were able to draw on the recently published Computer Science Curricula, produced by the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) [11]. The subject areas specified within this were adopted for use in the undergraduate certification framework without modification. Consideration was, however, given to the level/depth of coverage that would be expected for each topic, depending upon whether the degree concerned had computer science or cyber security as its main focus, and whether it was at Bachelor's or Integrated Master's level. Table 1 again lists the main subject areas, noting that the ACM specification presents further details, with each area having an associated list of indicative topics coverage.

An assessment of existing postgraduate cyber security degrees in the UK revealed that while the majority would fit the classification of providing a general, broad foundation in the topic, there were nonetheless a range of more specialised degrees to be found. A survey of the market conducted in mid-2014 revealed multiple universities offering degrees in each of the following areas of specialisation:

- computer network and Internet security;
- digital forensics;
- human factors of security;
- secure systems design and development;
- security and risk management.

Of these, digital forensics and network security were the areas in which a more sizeable number of degrees could be identified, with at least six universities offering related degrees at Master's level, and further variants identified in undergraduate provision. As such, these areas were selected as a basis for specialised variants of the certification framework, with digital forensics added in 2014 and the network security specialisation added in 2016. In both cases, more specific work was required in order to determine and devise the core subject areas that related degrees would be expected to offer, and (unlike the computer science and general cyber security themes) there was no prior work that could be directly adopted or adapted. As such, it was necessary to determine the key subjects for each theme, and the underlying topics within them. This was done

in part by looking at good practice already represented within existing degrees, and then by supplementing by further expertise within the project team. The finalised sets of subjects were ultimately agreed through a process that again also involved extensive consultation and feedback with relevant external experts from industry, academia and government. The top-level subject structures are again presented in Table 1.

Table 1. Overview of top-level subject areas identified to support degree certification

Theme	Underlying Subject Areas
Computer Science *(areas adopted from ACM/IEEE)*	1. Algorithms and complexity; 2. Architecture and organisation; 3. Discrete structures; 4. Programming languages; 5. Software development fundamentals; 6. Software engineering; 7. Systems fundamentals; 8. Security fundamentals; 9. Networks (1); 10. Operating systems (1); 11. Human-computer interaction; 12. Information management; 13. Secure programming; 14. Low level techniques and tools; 15. Networks (2); 16. Systems programming; 17. Operating systems (2); 18. Embedded systems; 19. Social issues and professional practice.
Cyber Security *(areas adapted from IISP)*	A. Information Security Management (Policy, Strategy, Awareness and Audit; Legal and Regulatory Environment); B. Information Risk Management (Risk Assessment and Management); C. Implementing Secure Systems (Security Architecture; Secure Development); D. Information Assurance Methodologies and Testing (Information Assurance Methodologies; Security Testing); E. Operational Security Management (Secure Operations Management and Service Delivery; Vulnerability Assessment); F. Incident Management (Incident Management; Forensics). H. Business Continuity Management (Business Continuity Planning and Management); I. Information Systems Research (Research); J. Professional Skills.
Digital Forensics	I. Foundations of Digital Forensics; II. Digital Forensic analysis; III. Digital Forensic practice; IV. An application of Digital Forensics; V. Legal Process; VI. Information security; VII. Evidence handling and management.
Computer Network and Internet Security	1. Computer Networks; 2. Cyber Security; 3. Computer Network Security Threats and Attacks; 4. Computer Network Security Operations and Safeguards; 5. Computer Network Security Administration and Management; 6. Information Security and Risk Management.

It is important to note that none of themes within the certification framework sought to prescribe specific syllabi, in terms of what the degrees should actually teach and assess for each topic. Instead each of the subject areas and skills groups were supported by means of indicative topics that degrees would be expected to address if they were to claim that the area was covered. An illustrative example is presented in Fig. 1, expanding upon the Information Security Management discipline area (and its associated skills groups) from within the Cyber Security theme.

The first call for applications for certification, addressing universities offering general Master's in cyber security was launched in March 2014. The programme was then progressively expanded, with more degree themes being included and broadening the

focus beyond solely considering (postgraduate) Master's degrees. At the time of writing, the certification framework as a whole covers ten types of degree, split across Bachelor's, Integrated Master's and Master's levels, as listed in Table 2. For clarification, it is relevant to note that in the UK system Bachelor's and Integrated Master's degrees are undergraduate level degrees of typically three and four years of full-time study respectively (each of which may also be extended by a further year to incorporate an optional or mandatory placement year, depending upon the host institution). Meanwhile, UK Master's degrees are typically one year in duration, noting that the year in this case reflects the full calendar year, rather than incorporating the summer break that is found in traditional undergraduate study.

Security Discipline	**Skills Group**	**Indicative topic coverage**
A. Information Security Management *Principle: Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including polices, standards and guidelines), and cost-effective solutions (including impact of third parties) for information security within a given organisation).* *CESG Knowledge Requirements include:* • *Management frameworks such as ISO 27000 series* • *Legislation such as Data Protection Act* • *Common management Frameworks such as ISO 9000*	**i. Policy, Strategy, Awareness and Audit (A1, A2, A3, A5, G1)**	• The role and function of security policy • Types of security policy • Security standards (e.g. ISO/IEC 27000) • Security concepts and fundamentals • Security roles and responsibilities • Security professionalism • Governance and compliance requirements in law • Third party management • Security culture • Awareness raising methods • Acceptable use policies • Security certifications • Understanding auditability • The internal audit process
	ii. Legal & Regulatory Environment (A6)	• Computer Misuse legislation • Data Protection law • Intellectual property and copyright • Employment issues • Regulation of security technologies

Fig. 1. An extract from the certification guidance, showing a Cyber Security Discipline broken down into Skills Groups and indicative topic coverage

Table 2. NCSC certification options (as at May 2018).

Degree type	Degree themes/certifications	Typical duration and credits
Bachelor's	Computer Science for Cyber Security Computer Science and Cyber Security Computer Science and Digital Forensics	3-years / 360 credits
Integrated Master's	Computer Science for Cyber Security Computer Science and Cyber Security Computer Science and Digital Forensics	4-years / 480 credits
Master's	General Cyber Security Digital Forensics Computer Science for Cyber Security Computer Network and Internet Security	1-year / 180 credits

While most of the resulting degree themes are self-explanatory from the titles, it is worth making the distinction between what is meant by 'Computer Science *for* Cyber Security' as opposed to 'Computer Science *and* Cyber Security'. The latter case is where a degree (at undergraduate level) provides a comprehensive foundation in core computer science content, and accompanies it by a significant focus upon cyber security topics (with the study balance typically changing from computing towards cyber as the degree progresses). By contrast, the concept of computer science *for* cyber security is intended to reflect a degree (at undergraduate or postgraduate level) that substantially provides candidates with a deep knowledge of computer science topics (particularly system-level aspects – computer science areas 13 to 18 in Table 1), which is likely to serve them well later, in certain lower-level forms of activity in cyber security. Such degrees are still expected to have some specific cyber security coverage, but through a minority of credits and not necessarily to an advanced level. In setting up the undergraduate certification, it was our view that students studying cyber security required a strong foundation in underpinning computer science – hence the adoption of the ACM/IEEE Computing Curricula.

The topic focus (and consequent balance of taught credits) is expected to vary according to the theme and level of the degree concerned. Again, the framework is not prescriptive about the exact number of credits that needs to be associated with the delivery of each topic, but does indicate minimum levels and subject combinations according to the type of degree concerned. This is illustrated in Fig. 2, covering the ten degree types currently eligible for certification. For reference, 10 credits in the UK system is considered to equate to 100 hours of study, which may include lectures, tutorials, seminars, practical sessions, assessment, and independent study.

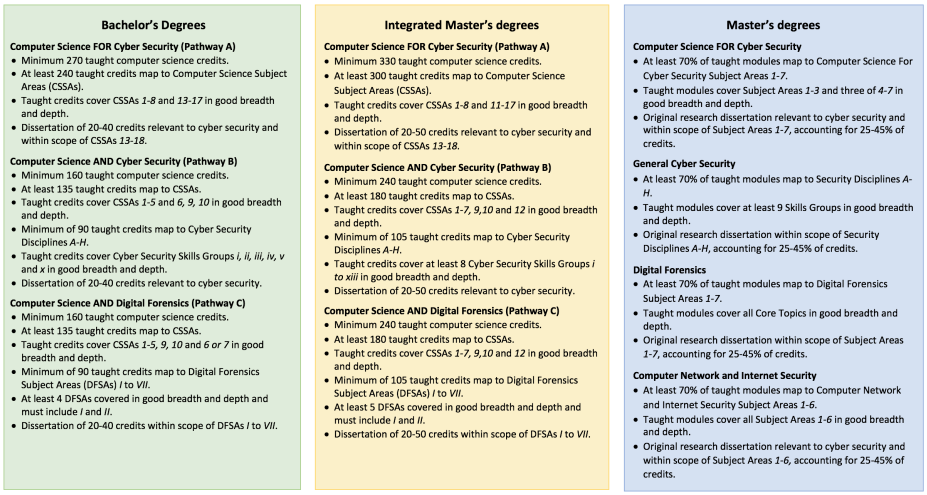

Fig. 2. A more detailed breakdown of the distribution and balance of credits between topics areas and levels of study across the different degree types.

4 The degree certification process and uptake

The certification process itself involves an extensive application being written for candidate degrees, and a rigorous review of resulting submissions. To gain full certification applications are required to address the following:

1. Evidence of institutional support (a letter from the Vice-Chancellor confirming commitment to the delivery of the degree);
2. Description of the applicant (e.g. the team delivering the degree and the resources to do so, linkage with industry, supported by CVs of key staff);
3. Description of the degree (e.g. the structure and content);
4. Assessment materials (e.g. approach to assessment, supported by examples of coursework that has been set for students and examinations used across the degree);
5. Individual Projects and Dissertations (e.g. the process of assessment and examples of assessed materials);
6. Student numbers and grades achieved (showing the entry and exit profiles of candidates studying on the degree).

Depending upon their preference and the maturity of their degrees, applicants are able to apply for either full or provisional level of certification. To be eligible for the former, a degree must have been running in both the previous and current academic year. Meanwhile, a degree seeking provisional certification does not need to have started yet, or may be running (for the first time) in the current academic year. Provisional applications are judged upon a reduced set of criteria, insofar as there is no assessment of student dissertations or the profile of students entering or graduating from the degree. To give a sense of the extent of resulting applications, those for Master's degrees are typically in the region of 100-150 pages (excluding any dissertation copies), while undergraduate applications can exceed 400 pages due to the greater volume of assessment and degree content materials being included.

All submissions are subject to a panel-based evaluation, encompassing representatives from academia, industry and government with cyber security knowledge and expertise. The panel is led by an independent Panel Chair and panel members typically review 3-5 applications. A full panel typically numbers around 12-15 persons (depending on the number of applications received). Prior to the panel, each submission is read and evaluated by three designated panel members (typically involving one from each of the aforementioned sectors, in all cases avoiding any conflicts of interest with the degree or university under consideration). The applicants are then scored on the basis of areas 2-6 above, according to the level of evidence provided (with 0 for no evidence, through to 4 for excellent evidence. Note that the institutional support letter is not graded, but must be present). Each section must achieve a threshold score of 3 (good evidence) in order for the certification to be awarded. Full certification typically lasts for 5 years, while the provisional level is typically valid for around 2 years (or until the first graduating cohort from the degree).

The response to the launch of the programme was very positive, and has continued to build and sustain interest as awareness has grown in the sector, and as further certification routes have been added to the portfolio. Fig. 3 illustrates the overall uptake of

the programme since launch, as well as the extent to which applications to date have been successful (noting that there is no quota for the number of certifications that can be awarded, and all applications are assessed entirely on their merits). The 2014 applications were exclusively for the certification of general Master's in cyber security. As the time goes on, however, the underlying data also includes a progressively wider mix of the other degree types and levels, as well as resubmission of applications for some degrees that were unsuccessful in earlier rounds (with many achieving success with their revised and strengthened versions). It should be noted that the apparent drop in 2018 is simply because this is based upon only partial data – reflecting the outcome of a Master's certification round, but not including the submissions for a subsequent Bachelor's call (for which the results were not known at the time of writing). Overall application numbers for 2018 are expected to be broadly similar to 2017, based on early indications from the current Bachelor's cycle. There is also a variation in terms of the proportion of degrees applying for full or provisional certification, with more of the applications in the more recent years tending towards the provisional route initially. Nonetheless, the programme has demonstrated a clear impact, and this appears likely to continue as the full range of certifiable degree routes becomes further established.

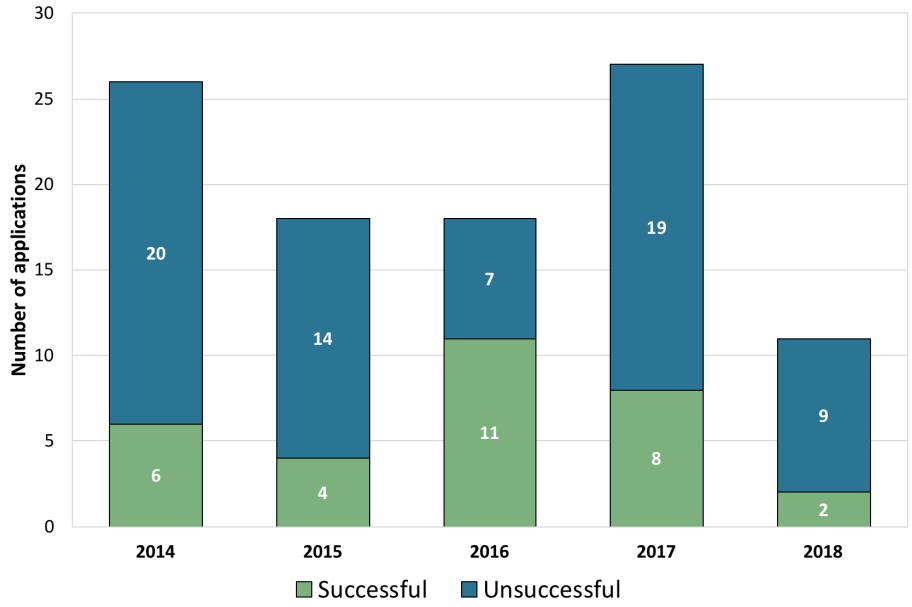

Fig. 3. Overall uptake of the certification programme, indicating the number of successful and unsuccessful applications per annum.

In addition, a number of further details have been established from the UK's Higher Education Statistics Agency in relation to the 2013/14, 14/15 & 15/16 academic years. Specifically, the number of UK nationals studying a Master's degree in cyber security has shown a healthy year-on-year increase over that period (from 260 to 460). Of these, the percentage studying a certified Master's degree has also shown a healthy increase

(from 34% to 51%), so that of those UK nationals who choose to study a Master's in cyber security, the majority now choose a certified degree. This is again indicative of significant positive impact from the programme as a whole, and individual universities have reported positive recruitment effects as a result of gaining the certification.

5 Lessons learned

With the overall certification and assessment process now having run for several years, it is possible to reflect upon a number of lessons learned. In terms of overall feedback from those directly involved, the assessors and panel chairs involved have consistently confirmed it is a very rigorous and fair process, and that a high bar has been set in terms of degree quality. Consensus on scoring has been good throughout, suggesting that the certifications and underlying criteria have been defined in a suitable manner and are effective in enabling assessors to understand the expected quality and identify whether it exists within the degrees.

The basic structure of the certification and the elements assessed (i.e. considering the academic team, degree content, assessments, dissertations, and student numbers) have also proven effective. Of these, the degree content is probably the most difficult and complex aspect for the panel to consider and evaluate. Assessments have flagged up a number of cases where this is heavily bookwork based and the process has been refined over the years to explicitly indicate that the ratio of bookwork to analysis would not be expected to exceed 60:40 at Master's level. Dissertations have proven very effective in providing an insight into the marking of students' work and provide good evidence of whether the students' work ultimately aligns with what the degree was positioning them to have learned.

The process has also demonstrated that universities are willing and able to benefit from the panel feedback. Over time, a number of submissions that initially failed to achieve the certification have returned in revised form (with associated modifications in terms of factors such as resourcing, content and/or assessment materials), and have then been successful. In these situations, the submissions have been revised in terms of more than just wording and presentation, and it is evident that the feedback has been helpful in guiding the academic teams in refining their degrees and/or enabling them to secure an increased level of support from their institutions.

Overall, it is clear that although the process demands excellence to be successful this has been achieved by a number of universities, and the number is growing.

6 Conclusions

The ongoing need for cyber security skills is likely to drive a corresponding demand for related academic degrees. This in turn creates an associated requirement for students and employers to have a means of identifying relevant and high-quality degrees that match the aspects of cyber security that they are interested in. In this context, the NCSC's certification programme has already made a notable contribution in the UK context. There has been demonstrable uptake of the approach, and feedback suggests that it has served to bring clarity and credibility to the degree landscape. Of course,

this does not mean that all uncertified cyber security degrees are lacking credibility, but it *does* mean that those with certification can be trusted. This simplifies matters for industry and employers looking to recruit appropriate graduates.

Moreover, the certification framework is now providing a basis against which new cyber security degrees are being designed. Indeed, the applications for provisional certification suggest an increase in the number of degrees seeking to address cyber security, and the structure of some of those now proposed (particularly at Master's level) has clearly been aided (or even driven) by the availability of the certification standards.

In the years since the certification work was initiated, other initiatives have also emerged that also seek to clarify the expectations of academic degrees in the security domain. A notable example in this context is the CSEC2017 Cybersecurity Education Curriculum [12], which aims to provide comprehensive cybersecurity curricular content at the post-secondary level and results from a two-year joint task force led by the ACM and the IEEE Computer Society, in collaboration with related groups within the Association for Information Systems and the International Federation for Information Processing. Moreover, the certification activity itself sits within a wider portfolio of NCSC-supported activities linked to academia. These also include support for Academic Centres of Excellence in Cyber Security Research, Academic Research Institutes, and Doctoral Studentships (see https://www.ncsc.gov.uk/Academics-and-researchers). Perhaps most notably, since starting the degree certification programme the UK's National Cyber Security Programme has begun to fund a project to identify and describe the foundational knowledge in cyber security – the Cyber Security Body of Knowledge (https://www.cybok.org). This work is being undertaken by a team of UK academics led by the University of Bristol, drawing on the expertise of international cyber security experts as authors and reviewers. The work has identified 19 cyber security Knowledge Areas grouped into 5 main categories: systems security; infrastructure security; software and platform security; human, organisational and regulatory aspects; attacks and defences [13]. Over the next few years, we anticipate that we will increasingly start to use the CyBOK as the reference for defining the content of cyber security degrees. This may lead to different 'flavours' of certified degrees depending on the content pathways chosen through the CyBOK.

Acknowledgements

We would like to thank the team of assessors and Panel Chairs who have worked with us over the past four years and without whom we would not have been able to set up the certification programme.

We would also like to thank Prof. Andy Jones from the University of Hertfordshire for his help in developing the content for Digital Forensics and Computer Network and Internet Security themes.

Student Record 2015/16; HESA Student Record 2014/15; HESA Student Record 2013/14; HESA DLHE Record 2015/16; HESA DLHE Record 2014/15; HESA DLHE Record 2013/14; HESA Student Record 2016/17; HESA DLHE Record 2016/17.

References

1. National Audit Office: The UK cyber-security strategy: Landscape review, 12 February 2013. www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/ (2013).
2. Center for Cyber Safety and Education: 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan Executive Briefing, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf (2017).
3. HM Government: National Cyber Security Strategy 2016-2021, 1 November 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (2016).
4. Cox, J: UK faces dramatic cyber-security skills 'cliff edge' and is chronically under prepared for hacker attacks, study finds, The Independent, 13 February 2017. https://www.google.co.uk/amp/s/www.independent.co.uk/news/business/news/uk-cyber-security-skills-cliff-edge-under-prepared-hacker-attacks-study-multinationals-government-a7578091.html (2017).
5. Martin, KM, Ciechanowicz, C, Piper, FC & Robshaw, MJB: Ten years of information security Master's programmes: reflections and new challenges. in Security Education and Critical Infrastructures: Proceedings of WISE03. Kluwer, pp. 215-230 (2003).
6. Furnell, S. Securing a good degree?, IISP Pulse, Issue 5, Spring 2011, pp6-8 (2011).
7. NSA: National Centers of Academic Excellence in Cyber Defense. 3 May 2016, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/ (2016).
8. ISO: Information technology – Security techniques – Code of practice for information security controls, ISO/ IEC 27002:2013. International Organisation for Standardisation, 1 Oct 2013. www. iso.org/standard/54533.html (2013).
9. (ISC)²: The (ISC)² CBK, https://www.isc2.org/Certifications/CBK#, last accessed 2018/5/10.
10. IISP: IISP Information Security Skills Framework, V6.3, July 2010, Institute of Information Security Professionals (2010).
11. CS2013: Computer Science Curricula 2013 - Curriculum Guidelines for Undergraduate Degree Programs in Computer Science, 20 December 2013, https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf (2013).
12. CSEC2017: Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Version 1.0 Report, 31 December 2017, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (2017).
13. Rashid, A., Danezis, G., Chivers, H., Lupu, E. and Martin, A: Scope for the Cyber Security Body of Knowledge, Version 2.0, 10 November 2017, https://www.cybok.org/media/downloads/CyBOKScopeV2.pdf (2017).